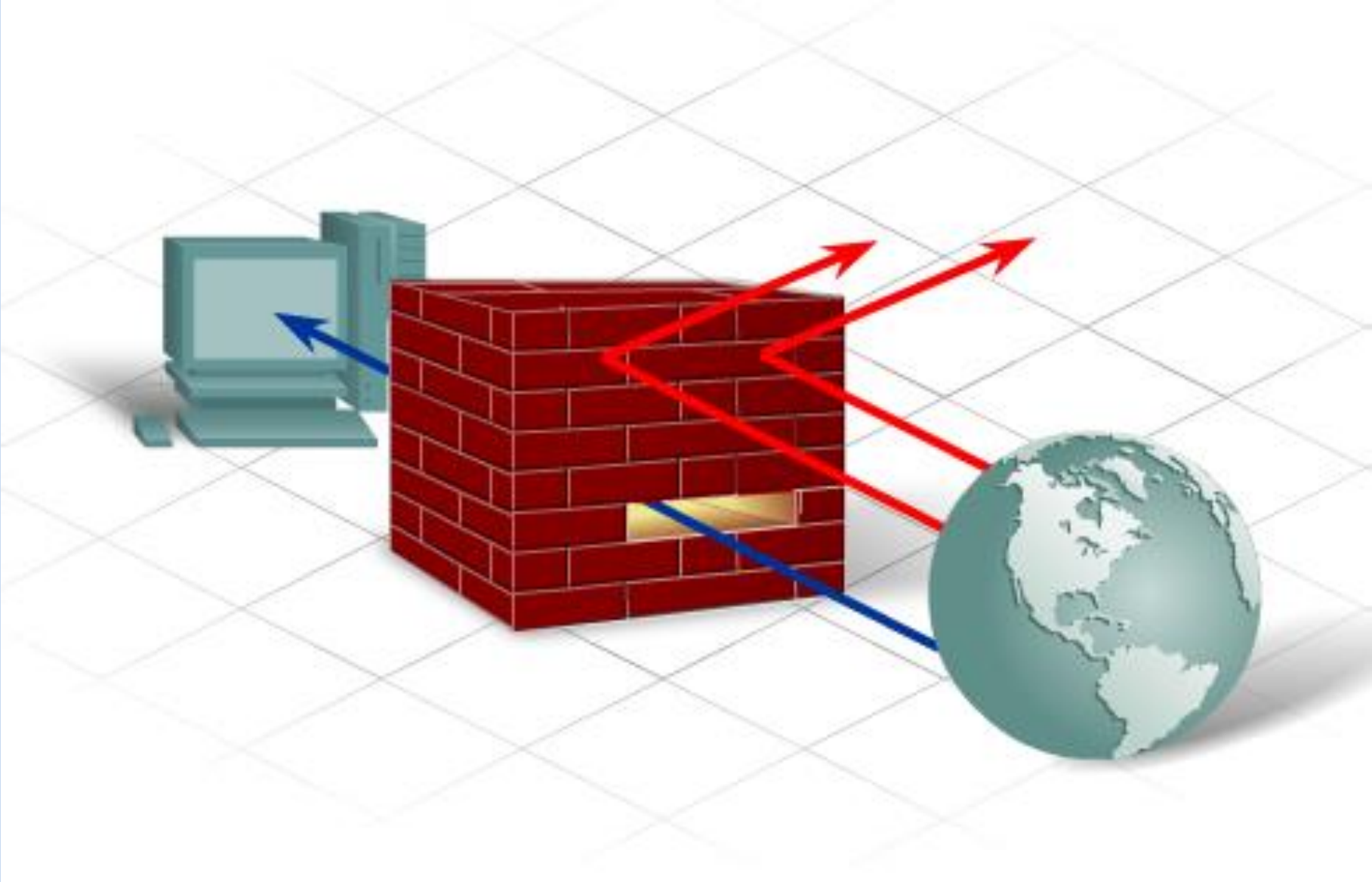
13. gyakorlat

Deák Kristóf

Tűzfal



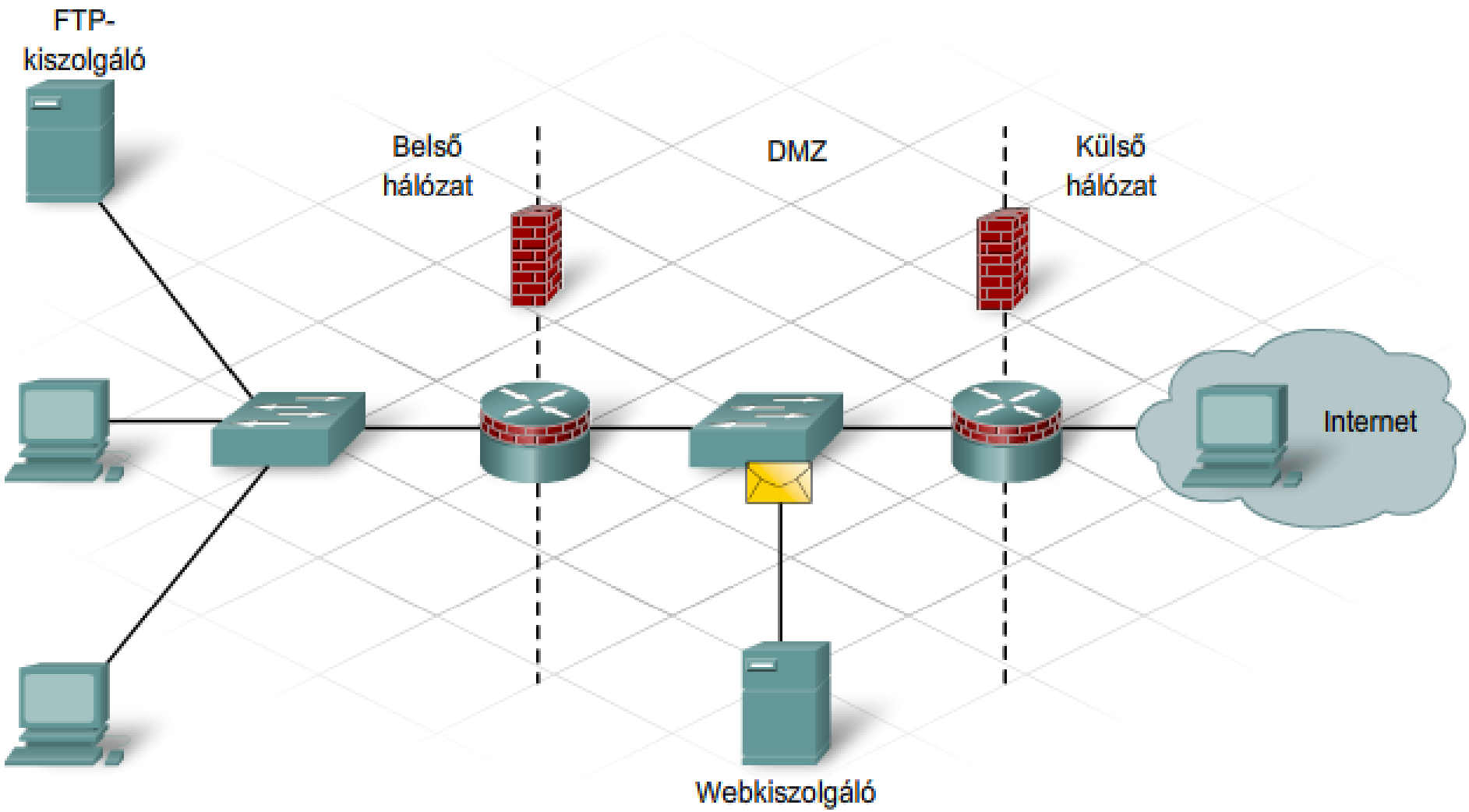
Miért kell a tűzfal?

- **Csomagszűrés** - az IP vagy MAC-cím alapján akadályozza meg vagy engedélyezi a hozzáférést.
- **Alkalmazás/Webhely szűrés** - Az alkalmazás alapján akadályozza meg vagy engedélyezi a hozzáférést. A webhelyek, egy meghatározott weblap URL címe vagy kulcsszavak alapján blokkolhatók.
- **Állapot-alapú csomagvizsgálat** (Stateful Packet Inspection, SPI) - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek. A nem kívánatos csomagokat külön engedély hiányában kiszűri. Az SPI felismerhet és kiszűrhet bizonyos típusú támadásokat is (pl.: DoS).

Tűzfal típusok

- **Eszköz-alapú tűzfal** - az eszköz-alapú tűzfal egy biztonsági készülékként ismert célhardverbe van beépítve.
- **Kiszolgáló-alapú tűzfal** - a kiszolgáló-alapú tűzfal egy tűzfalalkalmazás, amely valamilyen hálózati operációs rendszer alatt fut (Network OS: UNIX, Windows, Novell).
- **Integrált tűzfal** - az integrált tűzfal egy meglevő eszköz (pl.: forgalomirányító) tűzfalszolgáltatással kiegészítve.
- **Személyes tűzfal** - a személyes tűzfal a munkaállomáson helyezkedik el, nem LAN megvalósításra tervezték. Lehet az operációs rendszer beépített szolgáltatása, vagy származhat külső gyártótól is.

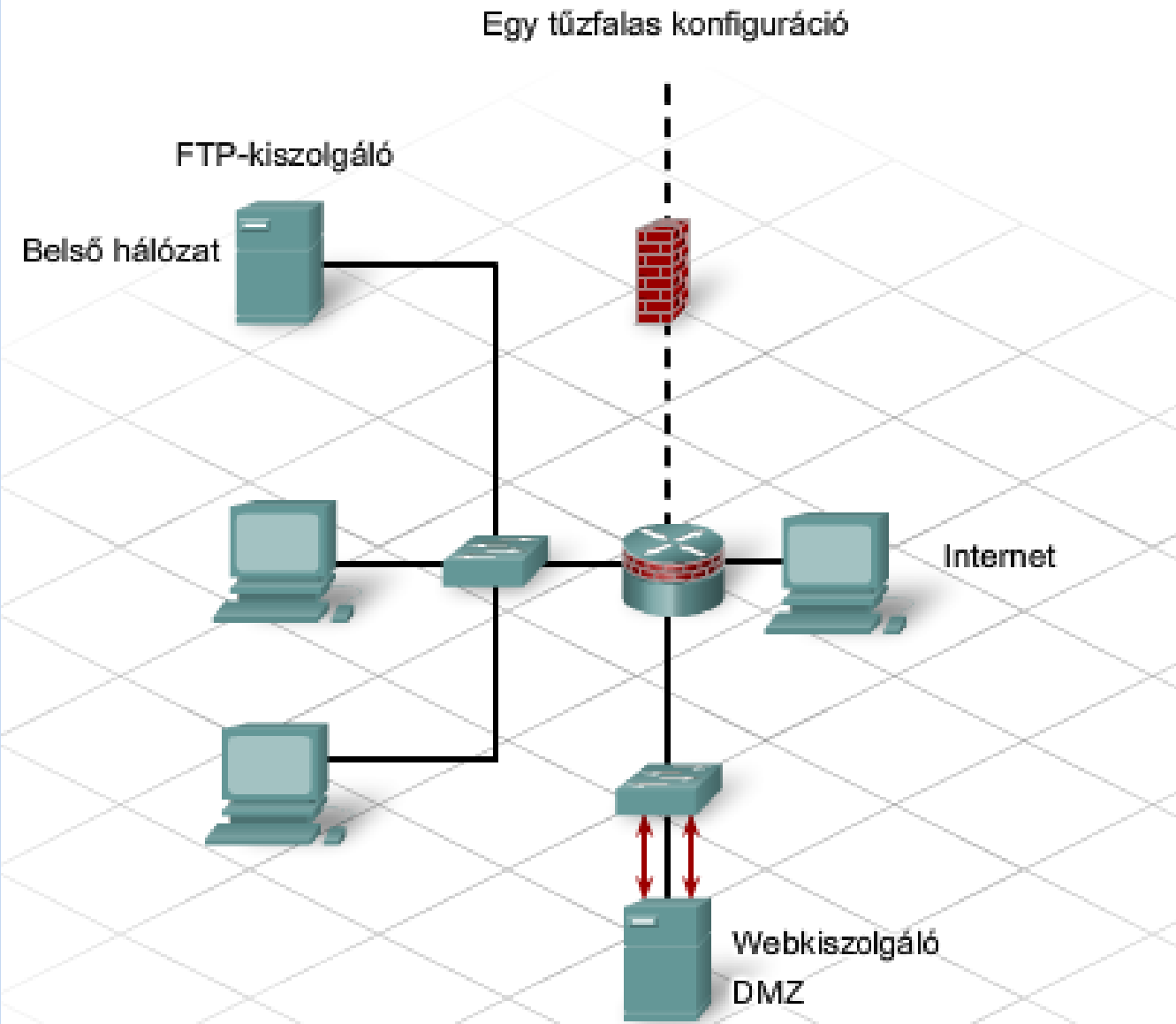
A tűzfal használata



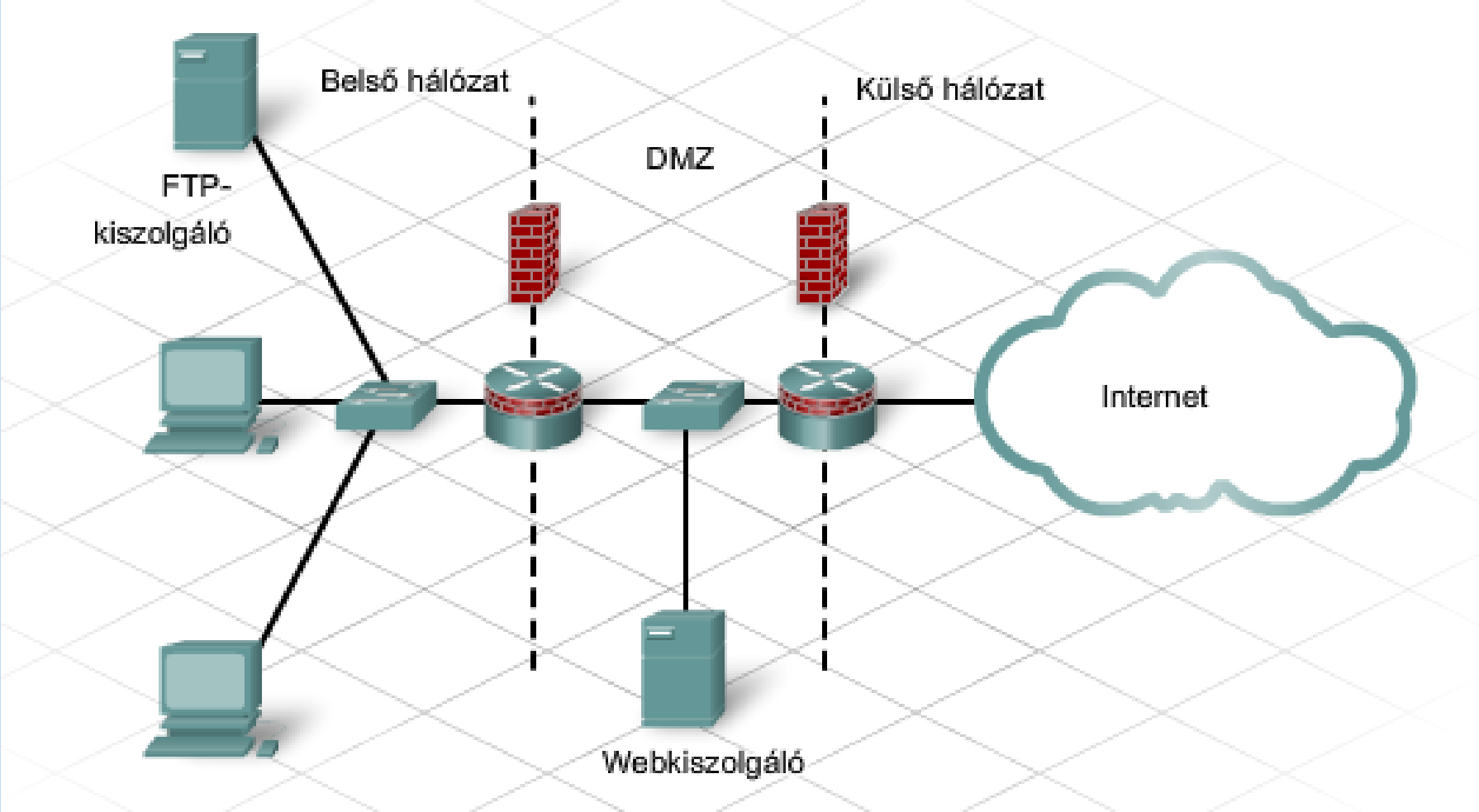
Demilitarizált zóna

- A demilitarizált zóna kifejezés a hadseregtől lett kölcsönözve, ahol a DMZ két haderő között kijelölt olyan terület, ahol tilos katonai tevékenység folytatása. A számítógépes hálózatok világában a DMZ a hálózat egy olyan területére vonatkozik, mely mind a belső, mind a külső felhasználók számára hozzáférhető. Biztonságosabb, mint a külső hálózat de nem olyan biztonságos, mint a belső hálózat. A belső hálózatot, a DMZ-t és a külső hálózatot egy vagy több tűzfallal különítik el. A nyilvános hozzáférésű webkiszolgálókat gyakran a DMZ-ben helyezik el.

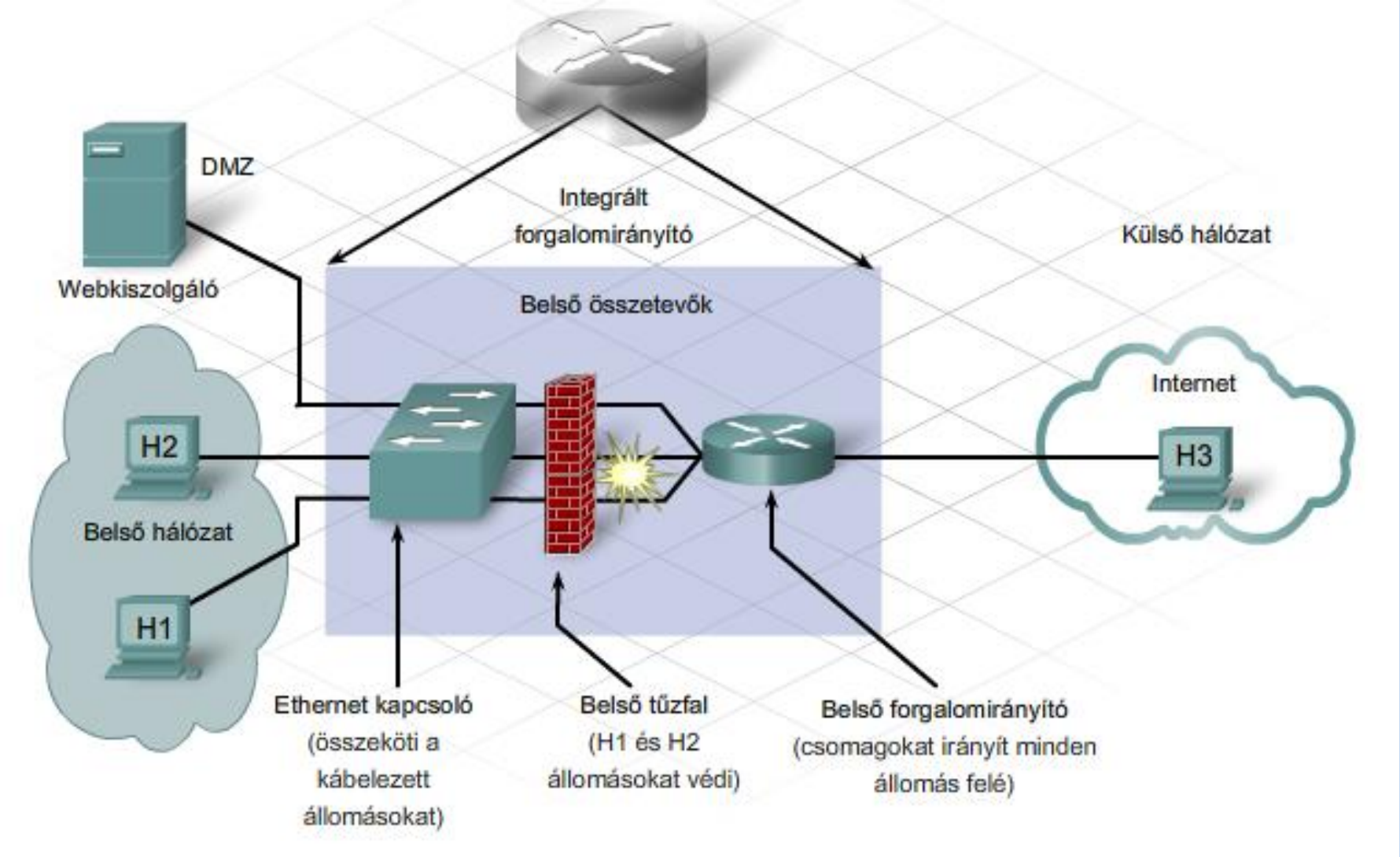
Egy tűzfalas konfiguráció



Két tűzfalas konfiguráció



A tűzfal felépítése



Tűzfal konfigurálás

- A gyakorlaton csomagszűrést fogunk használni, már egy jól ismert technológiával, a NAT-tal

<u>Csoportosítás:</u>

Külső tűzfal

- a teljes helyi hálózatot részben elválasztja az internettől

Belső tűzfal

- a helyi hálózatnak egy különösen védendő részét zárja el annak többi részétől (így az internettől is)
- Bármilyen tűzfalmegoldást alkalmazunk is, a szakma által elfogadott alapmódszer a következő: minden tilos, kivéve, amit szabad. A vállalat igényeit pontosan ismerő rendszergazda sokat profitálhat abból, hogy pontosan csak annyit engedjen, amennyi feltétlenül szükséges.

Gyakorlati szabályok például

- a vállalat belső hálózatán levő számítógépek internet felé irányuló valamennyi kapcsolatépítése letiltva, kivéve: a 80-as, kvázi szabvány http porton a vállalat saját weboldalát. Ezt általában elegendő az internetvonal(ak) megosztását (NAT) végző gépen tűzfalszabályként alkalmazni.
- a vállalat belső hálózatán levő számítógépek internet felé irányuló valamennyi kapcsolatépítése letiltva, kivéve: a 80-as http porton és 443-as biztonságos https porton tetszőleges weboldal. Ezt szintén elegendő a NAT-olást végző gép(ek)en tűzfalszabályként alkalmazni.
- a vállalat belső hálózatán levő számítógépek internet felé irányuló valamennyi kapcsolatépítése letiltva, kivéve egyes szolgáltatásokat, mint a http(s), dns, pop3, smtp, egyebek. Ezt a NAT-olást végző számítógépen az egyes szolgáltatásokhoz tartozó kimenő portok engedélyezésével tehetjük meg.
- a vállalat belső hálózatán levő számítógépek egymás közötti hálózati kapcsolatépítésének korlátozása csak engedélyezett szolgáltatásokra: ilyenkor vagy vállalati switchen kell csomagszűrést alkalmazni (például a gépek között mindent letiltunk, kivéve a 137, 138, 139 portokat a fájlmegosztások elérésére), vagy ugyanezt a módszert minden egyes számítógépen alkalmazni kell egy tűzfalprogrammal.

ACL parancsok

- **permit** - engedélyezés a további feltételek egyezése esetén a csomag továbbításra kerül.
- **deny** - tiltás a további feltételek egyezése esetén a csomag eldobásra kerül.
- **remark** - megjegyzés. Akár több megjegyzés sort tűzhetünk az Acl sorok közé.
- **dynamic** - dinamikus lista.

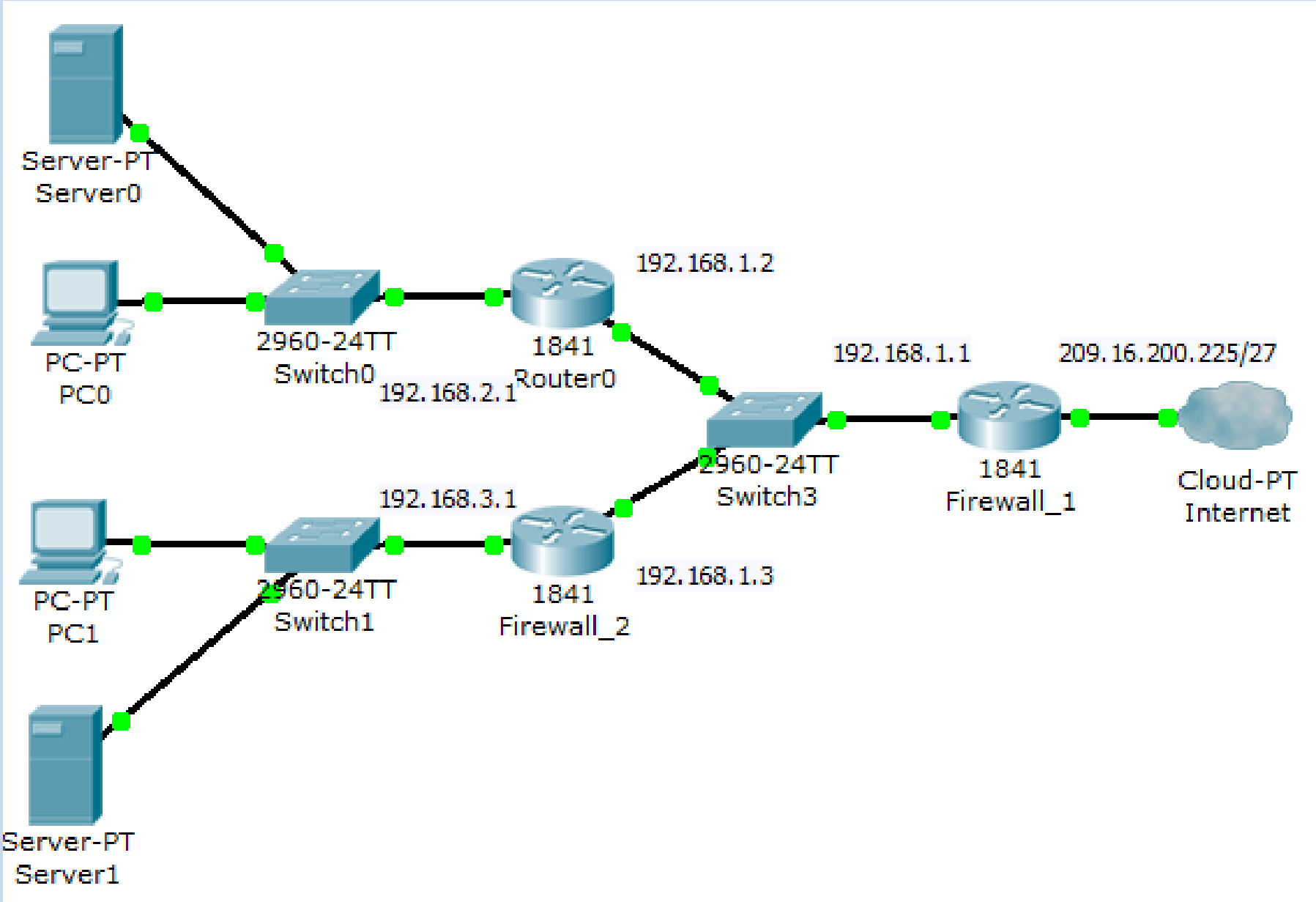
Csomag típusok

- **0-255** protokoll szám
- **ahp** Authentication Header Protocol
- **eigrp** EIGRP routing protocol
- **esp** Encapsulation Security Payload
- **gre** GRE tunneling
- **icmp** Internet Control Message Protocol
- **igmp** Internet Gateway Message Protocol
- **igrp** IGRP routing protocol
- **ip** Internet Protocol
- **ipinp** IP in IP tunneling
- **ipv4** Ipv4 verzió
- **ipv6** Ipv6 verzió
- **nos** NOS IP over IP tunneling
- **ospf** OSPF routing protocol
- **pcp** Payload Compression Protocol
- **pim** Protocol Independent Multicast
- **tcp** Transmission Control Protocol
- **udp** User Datagram Protocol

ACL címzések

- **any** - Minden cím
- **192.168.1.0 0.0.0.255** - egy **C** osztályú tartomány
- **128.0.0.0 15.255.255.255** - Osztálymentes tartomány
- **host 152.14.11.33** - -egyetlen Ip cím
- **any eq 23** - minden cím amely 23-as portot szólít meg.
- **any gt 100** - minden cím amely a 100-nál nagyobb portot szólít meg.
- **any lt 100** - minden cím amely a 100-nál kisebb portot szólít meg.
- **any range 100 199** - minden cím amely a 100 és 199 közti portot szólít meg.

Gyakorlati példa



1. szituáció: A hálózat védelme hekker támadásokkal szemben

- Mivel a biztonság a vállalat érdeke, a hálózat védelmére tűzfalat ajánl az internetes támadásokkal szemben. A hálózat internetről történő elérésének szigorítása elengedhetetlen.
- A szükséges beállításokat adjuk meg a Firewall 1 tűzfalon

Parancsok

Router(config)#access-list 100 deny ip any host 209.165.200.225

Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255

Router(config)#ip nat inside source list 1 interface FastEthernet0/0 overload

Router(config)#interface fastEhternet 0/1

Router(config-if)#ip access-group 100 in

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip nat inside

- **2. szituáció:**
- Most, hogy a teljes hálózat védelme biztosítva van az Internetről kiinduló forgalommal szemben, a kutatási és fejlesztési Subnet C hálózatot kell megvédeni a lehetséges belső hálózatról származó szabálysértések ellen. A kutatási és fejlesztési csoportnak hozzáférésre van szüksége Subnet B hálózathoz és az internethez egyaránt a kutatás vezetéséhez. A "B" alhálózat állomásai számára meg kell akadályozni a hozzáférést a kutatási és fejlesztési csoport alhálózatához.
- A szükséges beállításokat adjuk meg a Firewall 2 tűzfalon

Parancsok

Router(config)#access-list 100 permit ip host 192.168.2.10 any

Router(config)#access-list 100 permit ip host 192.168.1.1 any

Router(config)#access-list 100 permit ip host 209.165.200.225 any

Router(config)#access-list 1 permit 192.168.3.0 0.0.0.255

Router(config)#ip nat inside source list 1 interface FastEthernet0/1 overload

Router(config)#interface fastEthernet0/0

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#interface fastEthernet0/1

Router(config-if)#ip access-group 100 in

Router(config-if)#ip nat outside

Jegyzőkönyvhöz

- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml
- http://blog.szollosi.net/index.php/2008/09/23/cisco-natpat/

Köszönöm a figyelmet!

Sikeres vizsgaidőszakot mindenkinek!